LLNL-CONF-679241

Simple Institutional and User Best Practices for Cybersecurity in Research Reactors

G. K. White

November 12, 2015

IAEA International Conference on Research Reactors
Vienna, Austria
November 16, 2015 through November 20, 2015

Disclaimer

This document was prepared as an account of work sponsored by an agency of the United States government. Neither the United States government nor Lawrence Livermore National Security, LLC, nor any of their employees makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States government or Lawrence Livermore National Security, LLC. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States government or Lawrence Livermore National Security, LLC, and shall not be used for advertising or product endorsement purposes.

Simple Institutional and User Best Practices for Cybersecurity in Research Reactors

Greg White
Lawrence Livermore National Laboratory
November 2015

Abstract

As industrial control, physical protection, and material control and accounting systems continue to be converted to computer- and network-based systems, they are becoming more interconnected and complex. In addition, these systems have a much longer operational life than traditional desktop and server computer systems. Because of operational constraints, however, these systems are often patched far less frequently, and their state-of-the-art computer security lags years behind current best practices for traditional information technology (IT) systems. We will discuss simple institutional and user best practices that can be applied to these systems to minimize risk.

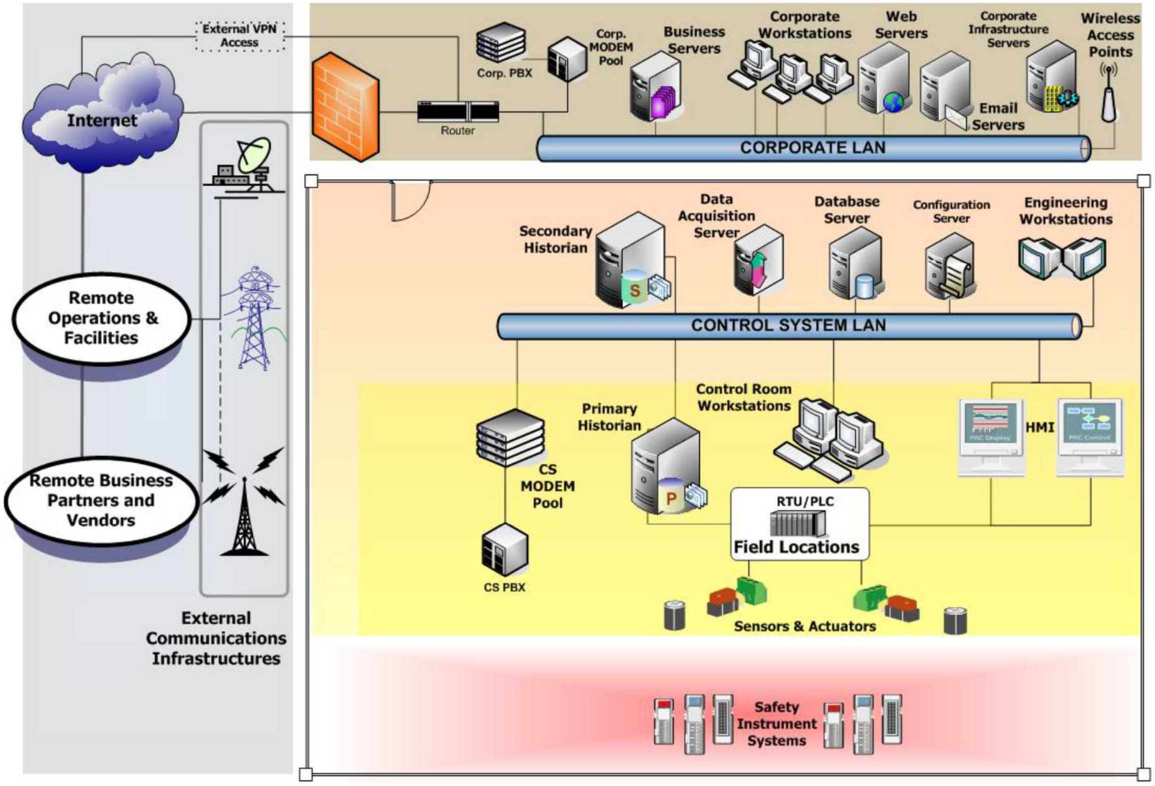
1 - Introduction

Managers of research reactors often have limited budgets to address differing and conflicting needs and requirements. These can take the form of research and operational needs, safety, and security. Cybersecurity spans all of these areas. This paper hopes to delineate some simple ideas to increase the cybersecurity posture of the facility.

2 – Institutional Best Practices

Security Policies: It is critical to have written computer security policies that are regularly updated and approved by all stakeholders. These policies should document all security policies, procedures, tools, and training, including what information and equipment is to be protected. The policies should also explain what constraints users have on their behavior and what barriers are in place to prevent adversaries from gaining access. Policies that are not documented or updated regularly are not enforceable or auditable. Unwritten cybersecurity measures tend to degrade in their implementation and effectiveness over time.

Network Separation and Access Control using Firewalls: In a perfect world, IT, industrial control systems (ICS), safety, and security systems would each exist on separate, air-gapped networks, with no remote access to the ICS, safety, or security systems. A network diagram of how this arrangement might look is shown below:



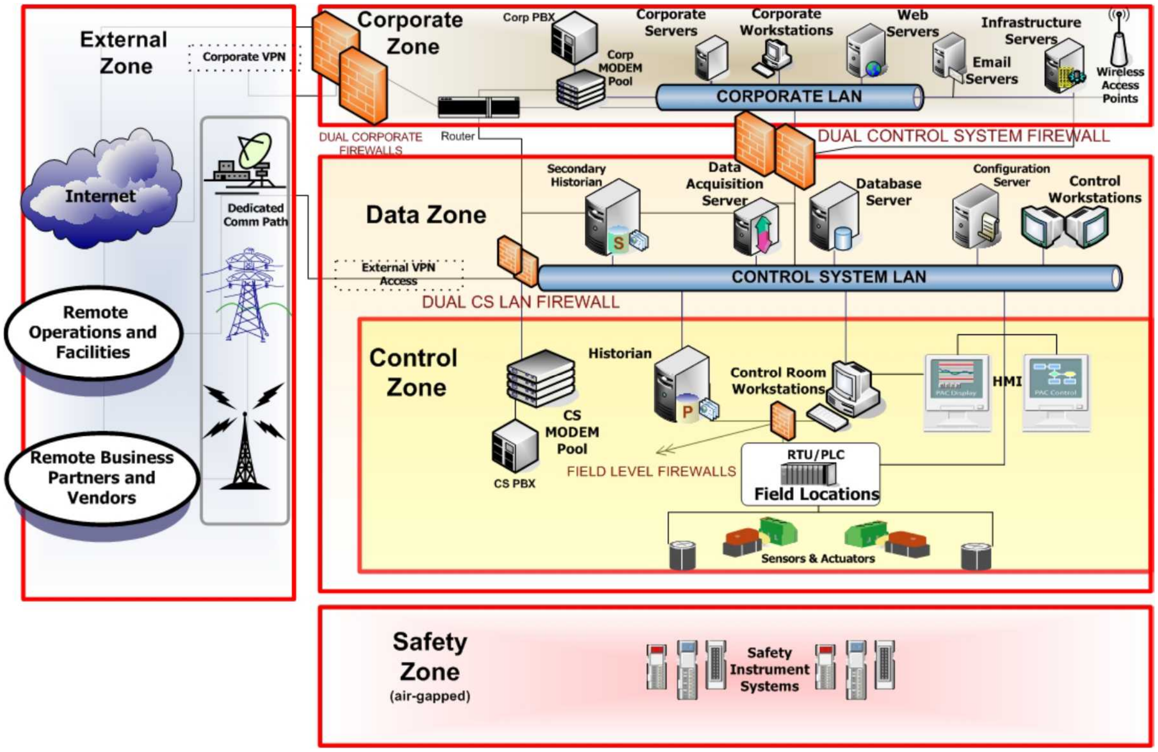
[1]

However, this is rarely the case. As systems age and become more complex, valid business reasons (and often less valid reasons such as convenience) sometimes exist to interconnect the networks or provide partners (e.g., academic partners, vendors, and users) access either remotely or from other networks. This is an important path by which malware or a third party can take control of your systems. The recent compromise of Target's credit card processing system was due to a spearfishing attack on one of Target's HVAC maintenance vendors. This gave the attackers passwords access to a billing system on Target's corporate network. The attackers then compromised the point of sale systems.[2]

If systems and networks are interconnected, then firewalls should be installed between your networks to limit communications between systems to only what is absolutely necessary. Firewalls should be configured with a "default deny" policy—that is, blocking all information transfers that are not specifically allowed by the firewall's rules. Below is a more secure network diagram with firewalls at key points:

[1] Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies, October 2009, Department of Homeland Security, https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Defense_in_Depth_Oct09.pdf

[2] http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/



[1]

Network Monitoring and Situational Awareness: Network-monitoring tools can help summarize the types, quantity, source, and destinations of traffic and help identify unusual activity that is not specifically blocked. This approach can also potentially identify data exfiltration from your facility and provide situational awareness of what is "normal" on your networks.

ICS Forensics: Many industrial control systems have integrated forensic capabilities. Understand and exercise the forensic capabilities on these systems regularly—prior to a real incident—to understand how they are used and what information they can provide.

Network Intrusion Detection and Prevention: Analyze both perimeter and inside network traffic to detect common attack signatures. This can help identify when attackers are probing your networks from offsite and when they have successfully penetrated your network, and reveal malicious activity that is completely contained inside your network.

Configuration Management and Rogue Device Detection: Configuration management is a system that lists every device, its internal configuration, and its software. This can help with patch management. Network hardware can be configured to block unknown or new devices on the network. This prevents rogue devices from being added to your network and can keep your configuration management database current.

Integration of Physical Security with Computer Security: Physical security is a vital component of your computer security program. Fortunately, the protection of nuclear material requires a higher level of physical security than most computer installations. Control physical access to your site, networks, and computers. Implement escort procedures for short-term visitors. Escorts should have an understanding of your facility and the computer systems that the visitor will be accessing. Networks should be physically contained within the facility. When procuring new equipment, include computer security in the evaluation process. This is especially critical with ICS equipment because of its long operational lifetime.

Change Management: Understanding and evaluating changes to your systems and networks are important parts of the operations of your research reactor. These changes should require a formal change-management process. Integrate the computer security implications of changes to your systems into your existing change-management process.

Password Management: Different Industrial control system components often have varying levels of security with regards to passwords. Where possible, enforce a robust password-management strategy requiring passwords to be strong and changed regularly. Consider implementing two-factor authentication for critical systems and privileged accounts, if technically possible. Limit password sharing.

Separation of Duties and Privilege Control: Software developers should not engage in system administration of your computer systems. Limit who has privileged accounts, and only use the privileged accounts for actions that require them. Document who has privileged accounts and on what systems they have them. Remove all computer accounts (especially privileged accounts) when they are no longer needed, especially when users no longer work at your facility.

Secure Coding Practices and Processes: Follow industry standards for all locally developed software. Where possible, work with external vendors to understand and evaluate their software development practices, along with their vulnerability-disclosure process. This can be especially effective when comparing vendors during the procurement process.

Recognizing that "Security by Obscurity" Is no Longer Valid: Control system software is not secure simply because it has a small distribution (i.e., is obscure). Overall, the ICS industry is behind traditional IT with respect to software vulnerabilities. For many years, it was assumed that air gaps and physical security lessened the need to provide robust computer security.

Staying Abreast of Current Trends in ICS and IT Security: Investing in your computer security personnel is an important part of your computer security program. Allow these personnel to regularly communicate with appropriate ICS vendors, attend general and ICS-specific computer security training and conferences, and examine relevant websites and mailing lists.

Device Locking: Where possible, block new storage (such as thumb drives) and network devices from being plugged in to critical computers. Storage devices can be a critical path by which malware and other attacks get around air gaps and firewalls. New network devices can provide unknown and insecure paths into your networks, bypassing your existing computer security infrastructure.

3 – Institutional Best Practices for IT Networks and Systems

Securing your traditional IT network will indirectly increase the security of your industrial control, physical protection, and safety systems and networks. Hackers can use your IT systems as a beachhead to launch attacks on your other networks and can use information stored on your IT systems to understand your people, business practices, operational procedures, and specific configurations of your systems and networks. Information about your organization can be used in spearfishing attacks or social engineering. Below are some additional suggestions that are specific to IT networks but which would also impact operations on other networks.

Vulnerability Assessments and Automated Network Scanning: Use both unprivileged and privileged scans of all IP addresses on your IT networks to detect vulnerabilities. This approach allows any found vulnerabilities to be quickly mitigated and can also help detect rogue network devices.

Host Intrusion Detection and Prevention: Install software on your IT systems to detect and report changes in critical files or entries in your system logs that indicate possible malicious activity.

Automated Patching: One of the most-used pathways for malware is a system that is not up to date on security significant patches. This includes both the operating system and any installed applications. Perform automated patch installation and tracking after appropriate testing. Block machines that are not properly patched, both from accessing the network and from remote access. On your ICS systems, you should not automatically install patches. Patches on these systems should be extensively tested and performed only during scheduled maintenance periods.

Virus Protection: Where possible, regularly scan all IT networks and machines for any files with virus signatures. Virus-infected machines can provide command and control or remote access to the hackers.

Internet Use and Vulnerabilities: Another pathway for malware is via the websites your users visit. The best defense against website malware is keeping your browsers up to date. You can further increase the security of web browsing by actively scanning web traffic for malware and blocking malicious websites. This can be accomplished with a web proxy server.

4 – User Best Practices

Your users are a significant component in an effective computer security program. Decisions about your computer security program always involve tradeoffs between their ease of use and the overall security of your systems and networks. This section will suggest some ways your users can help.

Creating a Computer Security Culture: Users of your facility are already trained on a wide range of nuclear safety and security topics. Including a computer security component in required training is also important. All personnel must understand how the secure operation of systems can be enhanced or compromised by their own individual actions.

Countering Spear Phishing and Social Engineering: Train users to recognize and report spear phishing emails. Incorporate awareness of social engineering tactics and operational security into training.

Prohibiting Personal Devices: Technically and administratively prohibit users from connecting personal or contractor devices and computers to your safety, security, or ICS networks. Instead, use guest networks or provide USB charging stations, for instance.

Enforcing Security Requirements: Enforce minimum security requirements on any machines connecting to IT networks. For example, prohibit operating systems no longer supported by the vendor, such as Windows XP.

Data Protection and Encryption: For mobile or portable devices, all institutional data should be encrypted at rest. This can be accomplished using hardware- (i.e., self-encrypting hard drives) or software-based encryption. Both encryption methods should be standards compliant (similar to FIPS-140-2 in the U.S.). Provide users with encrypted disks and USB thumb drives.

Lawrence Livermore National Laboratory is operated by Lawrence Livermore National Security, LLC, for the U.S. Department of Energy, National Nuclear Security Administration under Contract DE-AC52-07NA27344.

This document was prepared as an account of work sponsored by an agency of the United States government. Neither the United States government nor Lawrence Livermore National Security, LLC, nor any of their employees makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States government or Lawrence Livermore National Security, LLC. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States government or Lawrence Livermore National Security, LLC, and shall not be used for advertising or product endorsement purposes.